107

Représentations et caractères d'un groupe fini d'un $\mathbb{C}$-ev. Exemples.

Cadre : G un groupe fini d'ordre n et V un $\mathbb{C}$-ev de dimension finie

I- Outils théoriques

1/ Représentation

[Rauch38]

Déf 1 : On appelle <u>représentation linéaire</u> d'un groupe G la donnée d'un espace vectoriel V et d'un morphisme de groupe $\rho : G \to GL(V)$.
La <u>dimension de la représentation</u> est la dimension du $\mathbb{C}$-ev V.

[COL117]

Ex 2 : * l'inclusion du groupe orthogonal $O(d)$ dans $GLd(\mathbb{R})$ fait de $\mathbb{R}^d$ une représentation de $O(d)$
* $\mathbb{C}$ est une représentation de $\mathbb{Z}$ par l'intermédiaire du morphisme de groupes $\begin{array}{l}\mathbb{Z} \longrightarrow \mathbb{C}^* \\ n \longmapsto \lambda^n\end{array}$, on le note $C(\lambda)$.
$\dim(C(\lambda)) = 1$

Déf 3 : Si ρ est injectif, on dit que V est une représentation fidèle de G.

Notons : si $\dim(V) = d$ et si $(e_1, \dots, e_d)$ est une base de V, on note <u>$R_V(g)$ la matrice</u> de $\rho_V(g)$ dans la base $(e_1, \dots, e_d)$

2/ Caractère

[COL119]

Déf 4 : Le <u>caractère</u> χ_V de V est l'appl. $\begin{array}{l}G \longrightarrow \mathbb{C} \\ g \longmapsto tr(\rho_V(g))\end{array}$

On appelle <u>degré du caractère</u> χ_V l'entier $\chi_V(1) = \dim(V)$

Rmq 5 : Si $\dim(V) = 1$, alors le caractère est un morphisme de groupe de G dans $\mathbb{C}^*$

Prop 6 : χ_V est une fonction centrale

Rmq 7 : $\rho_V(g)$ est diagonalisable et ses valeurs propres sont des racines n-ièmes de l'unité.

Appl. 8 : $\forall g \in G \quad \chi_V(g^{-1}) = \overline{\chi_V(g)}$

3/ Construction de représentations

[COL120]

* Déf 9 : Soient V_1 et V_2 deux représentations de G
La représentation $\rho_{V_1 \oplus V_2}$ est appelée <u>représentation somme directe</u> et définie par :

$$\rho_{V_1 \oplus V_2} : \begin{array}{l} G \longrightarrow GL(V_1 \oplus V_2) \\ g \longmapsto ((v_1, v_2) \longmapsto (\rho_{V_1}(g)(v_1), \rho_{V_2}(g)(v_2)) \end{array}$$

Prop 10 : $\chi_{V_1 \oplus V_2} = \chi_{V_1} + \chi_{V_2}$

* Si X est un ens. fini muni d'une action de G donnée par $(g, x) \longmapsto g \cdot x$
Déf 11 : La <u>représentation de permutation</u> V_X est définie comme l'espace vectoriel V_X de dimension $|X|$, de base $(e_x)_{x \in X}$ muni d'une action linéaire de G, $g \cdot e_x = e_{g \cdot x}$

Prop 12 : $\chi_{V_X}(g) = |\{x \in X \,/\, g \cdot x = x\}|$

Ex 13 : En prenant $X = G$ et l'action par translation, on obtient une représentation appelée <u>représentation régulière</u> et notée V_G.
On a $\chi_{V_G}(1) = |G|$ et $\chi_{V_G}(g) = 0$ si $g \in G \setminus \{1\}$

* Soient V_1 et V_2 deux représentations de G et soit $u : V_1 \to V_2$ une application linéaire.
Déf 14 : On définit la <u>représentation $Hom(V_1, V_2)$</u> par
$\rho_{Hom(V_1,V_2)}(g)(u) = \rho_{V_2}(g) \circ u \circ \rho_{V_1}(g^{-1})$

Prop 15 : $\chi_{Hom(V_1,V_2)}(g) = \overline{\chi_{V_1}(g)} \times \chi_{V_2}(g)$

Rmq 16 : Si $V_1 = V$ et V_2 est la représentation triviale, la représentation $Hom(V_1, V_2) = Hom(V, \mathbb{C})$ est la <u>représentation du dual V^*</u> de V. On a $\chi_{V^*} = \overline{\chi_V}$

Déf 17 : On dit que deux représentations V_1 et V_2 de G sont <u>isomorphes</u> s'il existe un isomorphisme linéaire $u : V_1 \to V_2$ commutant à l'action de G ($u \circ \rho_{V_1}(g) = \rho_{V_2}(g) \circ u$)

CSQ 18 : * $\dim(V_1) = \dim(V_2)$
* $R_{V_1}(g) = T^{-1} R_{V_2}(g) T$ où $T \in GLd(\mathbb{C})$

Prop 19 : Si V_1 et V_2 sont isomorphes, alors $\chi_{V_1}(g) = \chi_{V_2}(g)$ $\forall g \in G$

II- Décomposition des représentations

1/ Représentations et caractères irréductibles

[COL124] Déf 20 : Une <u>sous-Représentation</u> de V est un sev de V stable par G.

X Ex 21 : Le sous-espace vectoriel $H = \text{vect}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$ est une sous-Représentation pour la représentation par permutation de S_4.

[COL124] Déf 22 : On dit que V est <u>irréductible</u> si V ne possède pas de sous-Représentation autre que 0 et V.
Un caractère irréductible est le caractère d'une représentation irréductible.

Rmq 23 : Toute représentation de dim 1 est irréductible.

Prop 24 : Il existe sur V un produit scalaire qui est invariant sous l'action de G : $\langle v_1 | v_2 \rangle_V = \frac{1}{|G|} \sum_{g \in G} \langle g \cdot v_1 | g \cdot v_2 \rangle$ où $\langle \cdot | \cdot \rangle$ est un p.s quelconque.

Théo 25 : (Maschke) Toute représentation de G est somme directe de représentations irréductibles.
Théo 25' : Lemme de Schur. (*) A la fin du plan

[COL128] Déf 26 : $Rc(G) = \{$ fonctions centrales $\}$
On munit $Rc(G)$ du ps $\langle \cdot | \cdot \rangle$ défini par $\langle \phi_1 | \phi_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\phi_1(g)} \phi_2(g)$

Théo 27 : (Frobenius) Les caractères irréductibles forment une base de l'espace des fonctions centrales.

2'/ Applications de ces deux thms principaux

Cor 28 : Le nombre de représentations irréductibles de G est égal au nombre de classe de conjugaison de G.

Cor 29 : Si V est une représentation de G, si $V = W_1 \oplus \dots \oplus W_k$ une décomposition de V en somme directe de représentat° irréductible et si $W \in Irr(G)$ alors le nombre m_W de W_i qui sont isomorphes à W est égal à $\langle \chi_W | \chi_V \rangle$.
En particulier, il ne dépend pas de la décomposition et $V \simeq \bigoplus_{W \in Irr(G)} \langle \chi_W | \chi_V \rangle W$

Appl. 30 : * Deux représentations V_1 et V_2 de G ayant les mêmes caractères sont isomorphes
* Une représentation V de G est irréductible ssi $\langle \chi_V | \chi_V \rangle = 1$.

Cor 31 : Si W est irréductible alors W apparait dans la Représentation régulière avec la multiplicité $\dim W$

Appl. 32 : * $\sum_{W \in Irr(G)} (\dim W)^2 = |G|$ (Formule de Burnside)
* Si $g \neq 1$, alors $\sum_{W \in Irr(G)} \dim(W) \chi_W(g) = 0$

III - Utilisation en pratique des tables de caractères

1'/ Définition et premiers exemples

Déf 33 : Soit $c = |\text{Conj}(G)|$. La <u>table de caractère</u> de G est un tableau $c \times c$ dont les coefficients sont les valeurs des caractères irréductibles sur les classes de conjugaison [CCO 13]

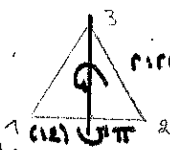
Prop 34 : Les colonnes du tableau sont orthogonales pour le produit scalaire $\mathbb{C}^c$ X

Ex 35 : * Table de $\mathbb{Z}/2\mathbb{Z}$ [CCO 13]

$\mathbb{Z}/2\mathbb{Z}$	1	-1
χ_1	1	1
χ_2	1	-1

* Table de $S_3 \simeq D_3$ [CRau 46]

S_3	1	$(1,2)$	$(1,2,3)$
χ_1	1	1	1
χ_ε	1	-1	1
χ_3	2	0	-1



rotation d'angle $\pm\frac{2\pi}{3}$ (312)

$\Rightarrow$ caractère associé à la représentation qui stabilise un triangle équilatéral

* Table de S_4 : (figure 1) **DVPT 1** [CPEY 228]

2'/ Détermination des sous-groupes distingués

Prop 36 : $K_{\chi_V} = \{ g \in G \ / \ \chi_V(g) = \chi_V(1) \} \triangleleft G$ [CPEY 231]

Prop 37: Les sous-groupes distingués de G sont exactement du type $\bigcap_{i\in I} K_{z_i}$ où $I \subset \{1,\dots,r\}$ r le nbr de caractère

Appl. 38: G est simple ssi $\forall i \neq 1$, $\forall g \in G$, $z_i(g) \neq z_i(1)$

[Rauch] 59 **Ex 39**: * Table de D_4

D_4	Id_1	$r^2{}_1$	r_2	s_2	sr_2
z_1	1	1	1	1	1
z_2	1	1	-1	1	-1
z_3	1	1	1	-1	-1
z_4	1	1	-1	-1	1
z_5	2	-2	0	0	0

le caractère associé à la représentation qui fixe un carré

Les sous-groupes distingués sont : D_4, K_4, $\mathbb{Z}/4\mathbb{Z}$, $\{Id\}$

X * Table de S_4 : S_4, $\mathcal{A}_4$, V_4, $\{Id\}$

3/ Cas des groupes abéliens

[COL 137] **Déf 40** : On note $\hat{G}$ le dual de G. Il est formé des morphisme de groupe de G dans $\mathbb{C}^*$

Théo 41 : G est abélien ssi toutes ses représentations sont de dimension 1.

[COL 134] DVPT2 **Théo 42** : Si G est un groupe fini commutatif, il existe $r \in \mathbb{N}$ et des entiers $N_1,\dots,N_r$ où N_1 est l'exposant de G et $N_{i+1} | N_i$ si $i \leq r-1$ tel que $G \simeq \mathbb{Z}/N_1\mathbb{Z} \times \dots \times \mathbb{Z}/N_r\mathbb{Z}$

X **Ex 43** : * Table de caractère de Klein $K_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

K_4	$(0,0)_1$	$(1,0)_1$	$(0,1)_1$	$(1,1)_1$
z_1	1	1	1	1
z_2	1	1	-1	-1
z_3	1	-1	1	-1
z_4	1	-1	-1	1

[PEY 4] * Table de caractère de $\mathbb{Z}/n\mathbb{Z}$. Notons $w = \exp\left(\frac{2i\pi}{n}\right)$

Les caractères sont $z_j : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}^*$, $k \longmapsto w^{kj}$

(Figure 2 en Annexe)

4/ Utilisation du quotient

Prop 44 : Soit $N \triangleleft G$ un sous-groupe distingué de G. Soit ρ_U une représentation de G/N sur un ev U. Alors il existe une représentation canonique de G sur U telle que les sous-représentations de U sous l'action de G/N soient exactement celles de U sous l'action de G. [PEY]

Prop 45 : Si ρ_U est irréductible, la représentation $\tilde{\rho_U}$ de G est aussi irréductible. X

Prop 46 : Notons $D(G)$ le groupe dérivé de G. Alors le nbr de représentation de dimension 1 est $|G|/|D(G)|$ [PEY]

Appl 47 : On peut obtenir des tables de caractères d'un groupe plus facile en utilisant la propriété 44.

* $D(\mathcal{A}_4) = K_4$ et $\mathcal{A}_4/K_4 \simeq \mathbb{Z}/3\mathbb{Z}$ [Rau 58]

On peut donc déduire de la table de $\mathbb{Z}/3\mathbb{Z}$ la table de $\mathcal{A}_4$ (Figure 3 en annexe)

* $D(D_4) = \{\pm 1\}$ et $D_4/\{\pm 1\} \simeq K_4$

On peut donc trouver la table de D_4

* $\mathbb{H} = \{\pm Id, \pm I = \pm i\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \pm J = \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm K = \pm i\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ [Rau 60]

et on a $I^2 = J^2 = K^2 = -Id$, $IJ = -JI = K$, $JK = -KJ = I$, $-IK = KI = J$

$D(\mathbb{H}) = \{\pm Id\}$ et $\mathbb{H}/\{\pm Id\} \simeq K_4$. On peut donc trouver la table de $\mathbb{H}$ (Figure 4 en annexe)

Rmq 48 : D_4 et $\mathbb{H}$ ont la même table de caractères mais ils ne sont pas isomorphes. (!) Rappel important

(*) **Théo 25** : (Lemme de Schur) Soient V_1 et V_2 deux représentations irréductibles de G.

1) Si V_1 et V_2 ne sont pas isomorphes, alors $Hom_G(V_1,V_2) = \{u \in Hom(V_1,V_2) \,/\, u \circ \rho_{V_1}(g) = \rho_{V_1}(g) \circ u\} = 0$
2) Si $V_1 = V_2$, alors $Hom_G(V_1,V_2)$ est la droite des homothéties

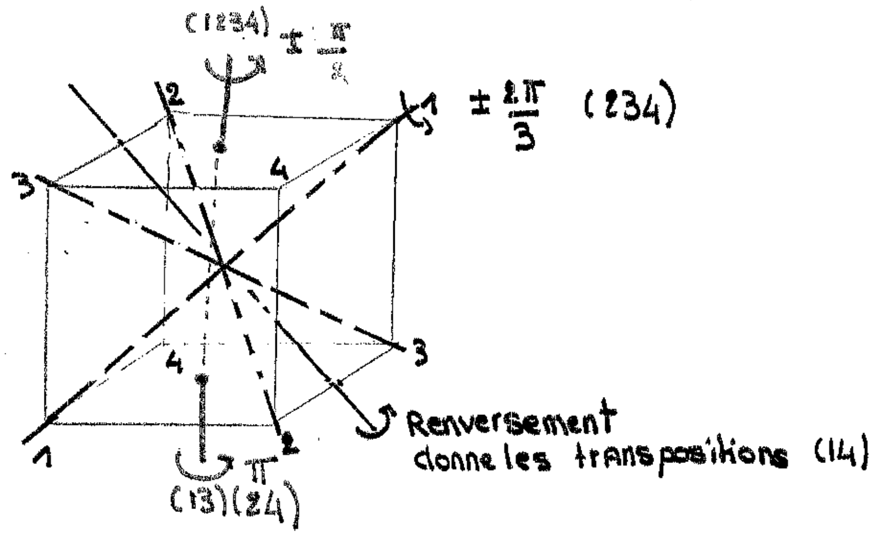
Annexe :

Figure 1 = Table de S_4

S_4	$[1111]_1$	$[211]_6$	$[31]_8$	$[22]_3$	$[4]_6$
χ_1	1	1	1	1	1
χ_ε	1	-1	1	1	-1
χ_T	3	1	0	-1	-1
χ_{cube}	3	-1	0	-1	1
	2	0	-1	2	0

← isométrie qui stabilise un tétraèdre

← isométrie positive qui stabilise un cube



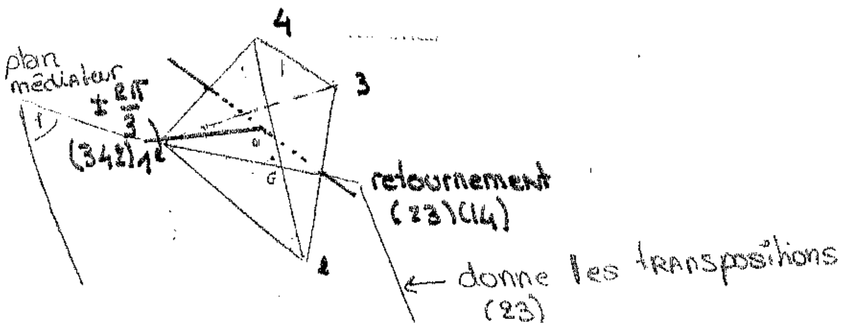


Figure 2 = Table de $\mathbb{Z}/n\mathbb{Z}$ [PEY]

$\mathbb{Z}/n\mathbb{Z}$	0_1	1_1	---	$(n-2)_1$	$(n-1)_1$
χ_1	1	1	---	1	1
χ_2	1	w		w^{n-2}	w^{n-1}
⋮	⋮	⋮		⋮	⋮
χ_{n-1}	1	w^{n-2}	---	$w^{(n-2)(n-2)}$	$w^{(n-2)(n-1)}$
χ_{n}	1	w^{n-1}	---	$w^{(n-1)(n-2)}$	$w^{(n-1)(n-1)}$

Figure 3 = Table de $\mathcal{A}_4$ [Rauch]

$\mathcal{A}_4$	$(1)_1$	$(123)_4$	$(132)_4$	$(12)(34)_3$
χ_1	1	1	1	1
χ_2	1	w	w^2	1
χ_3	1	w^2	w	1
χ_4	3	0	0	-1

Table de $\mathbb{Z}/3\mathbb{Z}$

➡ caractère associé à la représentation des isométries positives qui stabilise un tétraèdre régulier.

Figure 4 = Table de $\mathbb{H}$ [Rauch]

$\mathbb{H}$	Id_1	$-Id_1$	$\pm I_2$	$\pm J_2$	$\pm K_2$
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

[Rauch] RAUCH - Les groupes finis et leurs représentations

[PEY] PEYRE - L'algèbre discrète de la transformée de Fou

[COL] COLMEZ - Éléments d'analyse et algèbre

TABLE DE $\mathcal{S}_4$

Référence : PEYRÉ : Algèbre discrète de la transformée de Fourier p.229

THÉORÈME

La table de caractères de $\mathcal{S}_4$ est :

	$\boxed{1}$ (1)	$\boxed{6}$ (12)	$\boxed{8}$ (123)	$\boxed{6}$ (1234)	$\boxed{3}$ (12)(34)
χ_1	1	1	1	1	1
χ_ε	1	-1	1	-1	1
χ_s	3	1	0	-1	-1
$\chi_{\mathrm{Hom}(V_s,V_\varepsilon)}$	3	-1	0	1	-1
χ_5	2	0	-1	0	2

Preuve :

Classes de conjugaison

$\mathcal{S}_4$ possède 24 éléments repartis en 5 [1] classes de conjugaison [2]. En effet, il y a :
- Le neutre (1) seul dans sa classe.
- $\binom{4}{2} = 6$ transpositions (12)
- $2 \times \binom{4}{3} = 8$ 3-cycles (123)
- $3 \times 2 = 6$ 4-cycles (1234)
- $\frac{1}{2} \times \binom{4}{2} = 3$ double transpositions [3] (12)(34)

Représentation triviale

Elle est de dimension 1 car elle va dans $\mathbb{C}$. On note son caractère χ_1. Il vaut 1 tout le temps, on complète la première ligne.

Représentation alternée

Elle est de dimension 1 car elle va dans $\mathbb{C}$ et correspond au morphisme de signature ε. On note son caractère χ_ε. On complète la seconde ligne.

Représentation standard

(p. 203) Regardons la représentation naturelle de $\mathcal{S}_4$ sur $\mathbb{C}^4$ obtenue par permutation des vecteurs de base. Le caractère associé χ_{p} est la trace d'une matrice de permutation, c'est-à-dire le nombre de 1 sur la diagonale. Autrement dit $\chi_{\mathrm{p}}(\sigma)$ est le nombre de points fixes de σ. On a donc $\chi_{\mathrm{p}} = [4, 2, 1, 0, 0]$

Cette représentation laisse $H_0 = \mathrm{Vect}\{(1,1,1,1)\}$ stable. On note H_1 le supplémentaire de H_0. On a $H_1 = \{(x_1, \dots, x_4) \in \mathbb{C}^4 \ / \ x_1 + \cdots + x_4 = 0\}$.

Sur H_0, la représentation par permutations est la représentation triviale. On pose $\rho_s = \rho_{\mathrm{p}}|_{H_1}$ la représentation standard. Elle est dimension $3 = 4 - 1$. Il faut vérifier qu'elle est irréductible. Pour cela, on calcule son caractère :

$$\chi_s = \chi_{\mathrm{p}} - \chi_1 = [3, 1, 0, -1, -1]$$

Le calcul nous donne

$$\langle \chi_s, \chi_s \rangle = \frac{1}{24}\left(1 \times 3^2 + 6 \times 1^2 + 8 \times 0^2 + 6 \times (-1)^2 + 3 \times (-1)^2\right) = 1$$

χ_s est donc bien irréductible, on complète la troisième ligne.

1. Donc il y aura 5 caractères irréductibles
2. 2 éléments de $\mathcal{S}_4$ sont conjugués ssi ils sont de même type
3. à supports disjoints !

Les 2 dernières

On note n_4 et n_5 les degrés des 2 derniers caractères restants (on en a 3 et on sait qu'il y en a 5). Mais on sait que $\sum n_i^2 = 24$ donc $n_4^2 + n_5^2 = 24 - 1^2 - 1^2 - 3^2 = 13$. Les seuls solutions possibles sont 3 et 2.

L'avant dernière

On va regarder la représentation de morphismes donné par les représentations standard et alternée. On pose $\chi_{\mathrm{Hom}(V_s,V_\varepsilon)}$. On sait que le caractère va être de degré $3 \times 1 = 3$.

Par propriétés, on sait que $\chi_{\mathrm{Hom}(V_s,V_\varepsilon)} = \chi_s \overline{\chi_\varepsilon} = \chi_s \chi_\varepsilon$. On calcule (4ème ligne), ce caractère est bien différent des autres et on peut faire le calcul pour voir que $\langle \chi_{\mathrm{Hom}(V_s,V_\varepsilon)}, \chi_{\mathrm{Hom}(V_s,V_\varepsilon)} \rangle = 1$ ie la représentation est irréductible.

La dernière

On sait que le degré du caractère va être 2. On peut donc compléter $\chi_5((1)) = 2$. On remplit ensuite le reste de la ligne par orthogonalité des colonnes.

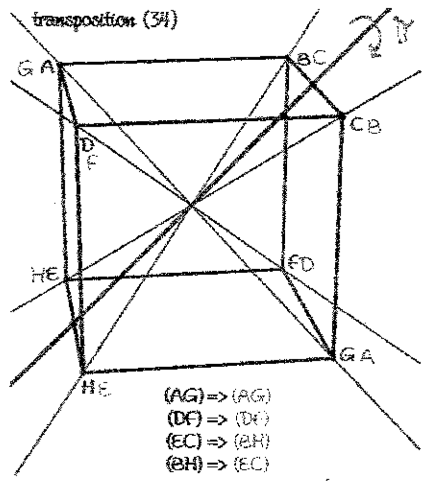
■

Vision géométrique pour $\chi_{\mathrm{Hom}(V_s,V_\varepsilon)}$ (Rauch p.47)

Une des réalisations de $\mathcal{S}_4$ est $\mathrm{Isom}^+(C_6)$. Pour cela on fait agir le groupe $\mathcal{S}_4$ sur les 4 diagonales du cube. On va noter χ_{cube} cette représentation.

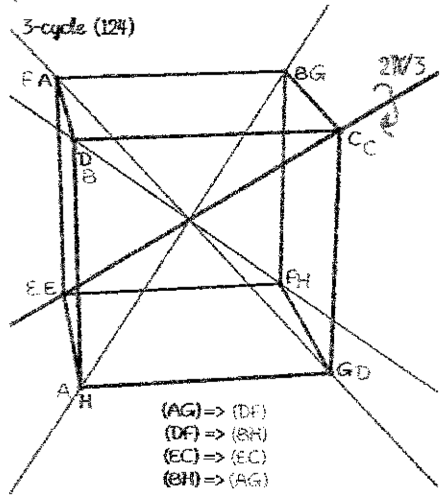
L'identité ...

$$\chi_{\mathrm{cube}}((1)) = \mathrm{tr}(\mathrm{Id}) = 3$$



Une transposition s'identifie à un demi-tour (angle $\pm\pi$) autour de la médiatrice commune à deux arêtes symétriques par rapport au centre du cube.

$$\chi_{\mathrm{cube}}((1)) = 1 + 2\cos(\pi) = -1$$

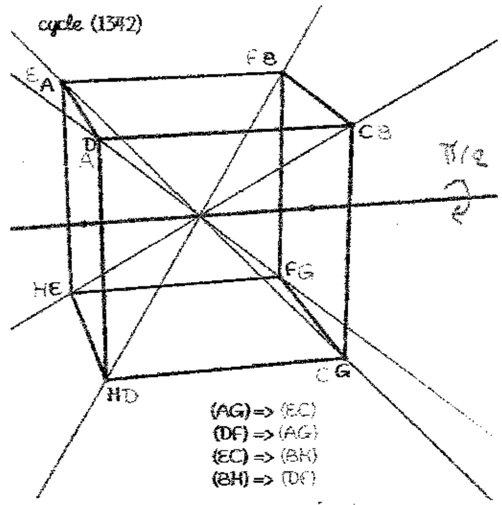


Un 3-cycle est identifié à une rotation d'angle $\pm\frac{2\pi}{3}$ autour de l'une des 4 diagonales du cube.

$$\chi_{\mathrm{cube}}((123)) = 1 + 2\cos\left(\frac{2\pi}{3}\right) = 0$$

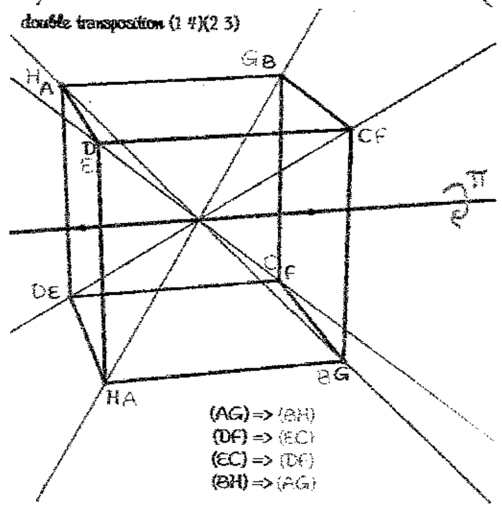
Un 4-cycle s'identifie à une rotation d'angle $\pm\frac{\pi}{2}$ autour de l'un des trois axes quaternaires du cube (axe passant par les centres de deux faces opposées)

$$\chi_{\text{cube}}((1234)) = 1 + 2\cos\left(\frac{\pi}{2}\right) = 1$$



Une double transposition est identifiée à un demi-tour (angle $\pm\pi$) autour de l'un des trois axes quaternaires du cube (axe passant par les centres de deux faces opposées)

$$\chi_{\text{cube}}((12)(34)) = 1 + 2\cos(\pi) = -1$$



On obtient bien $\chi_{\text{cube}} = \chi_{\text{Hom}(V_s,V_\varepsilon)} = [3,-1,0,1,-1]$.
On calcule $\langle \chi_{\text{cube}}, \chi_{\text{cube}} \rangle$ pour vérifier qu'elle est irréductible.

Notes :

✓ **A l'oral**, on ne peut mettre pas en lemme le fait que 2 éléments sont conjugués ssi ils ont même type (trop long). On fait les classes de conjugaisons directement sur la table. On remplit la table au fur et à mesure.
✓ **Temps :** feutre 11'. $\Rightarrow$ pour rallonger : table de $\mathcal{S}_3$ (Rauch) ou dire vision géométrique

Chapitre 46

Théorème de structure des groupes abéliens finis

Références : Colmez, *Éléments d'analyse et d'algèbre (et de théorie des nombres)*, p 250-252

On rappelle que l'exposant d'un groupe G est le plus petit entier n tel que pour tout $g \in G$, $g^n = e$. Comme pour tous g, $h \in G$, gh est un élément d'ordre $\text{ppcm}(o(g), o(h))$ **car G est abélien**, l'exposant est donc le ppcm des ordres des éléments du groupe, et aussi le plus grand des ordres des éléments du groupe.

Théorème.

Si G est un groupe abélien fini, alors il existe $r \in \mathbb{N}$ et des entiers N_1, ..., N_r, où N_1 est l'exposant de G et $N_{i+1}|N_i$ tels que

$$G \simeq \prod_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}.$$

Comme G est un groupe abélien fini, les classes de conjugaisons n'ont qu'un élément. On a donc $n = |G|$ représentations irréductibles de degré 1 par Burnside.
Puis on remarque que les caractères irréductibles sont des morphismes. Ce sont donc des éléments de $\widehat{G}$, le groupe abélien des morphismes de G dans $\mathbb{C}^*$.
Réciproquement, tout élément de $\widehat{G}$ fournit une représentation irréductible, donc un caractère irréductible.
$\widehat{G}$ est donc le groupe des caractères irréductibles de G.

Lemme.

On pose l'application

$$i : \begin{array}{ccc} G & \rightarrow & \widehat{\widehat{G}} \\ g & \mapsto & (\chi \mapsto \chi(g)) \end{array},$$

alors i est un isomorphisme de groupes.

Démonstration. i est bien un morphisme de groupes car les caractères sont des morphismes.
En effet,

$$i(gh)(\chi) = \chi(gh) = \chi(g)\chi(h) = i(g)(\chi)i(h)(\chi).$$

On a vu que $\widehat{G}$ est l'ensemble des caractères irréductibles. Il est donc de même cardinal que G. On a $\left|\widehat{G}\right| = \left|\widehat{\widehat{G}}\right|$, en appliquant le même raisonnement aux éléments de $\widehat{\widehat{G}}$, qui sont les caractères irréductibles sur $\widehat{G}$ **car $\widehat{G}$ est abélien.**
D'où $|G| = \left|\widehat{\widehat{G}}\right|$.
Il suffit de montrer que i est injectif.

Soit $g \in G$ tel que $i(g)(\chi) = 1 = i(e)(\chi)$. Alors $\forall \chi \in \widehat{G}$, $\chi(g) = \chi(e) = 1$.
On décompose $\mathbb{1}_{\{g\}}$ dans la base des caractères.

$$\begin{aligned}
\mathbb{1}_{\{g\}} &= \sum_{\chi \in \widehat{G}} \langle \mathbb{1}_{\{g\}}, \chi \rangle \chi \\
&= \sum_{\chi \in \widehat{G}} \frac{1}{G} \sum_{h \in G} \overline{\mathbb{1}_{\{g\}}(h)} \chi(h) \chi \\
&= \frac{1}{G} \sum_{\chi \in \widehat{G}} \chi(g) \chi \\
&= \frac{1}{G} \sum_{\chi \in \widehat{G}} \chi
\end{aligned}$$

On a donc en évaluant en e :

$$\mathbb{1}_{\{g\}}(e) = \frac{1}{G} \sum_{\chi \in \widehat{G}} \chi(e) = 1.$$

D'où $g = e$ et i est bien injective. □

Lemme.

G et $\widehat{G}$ ont même exposant.

Démonstration. Soit N l'exposant de G, on a $\forall \chi \in \widehat{G}$, $\forall g \in G$,

$$\chi^N(g) = \chi(g)^N = \chi(g^N) = \chi(1) = 1.$$

L'exposant de $\widehat{G}$ est inférieur ou égal à N.
On peut appliquer le même raisonnement à $\widehat{G}$ pour obtenir que N est inférieur ou égal à l'exposant de $\widehat{G}$ (car G et $\widehat{\widehat{G}}$ ont même exposant par le lemme précédent).
Cela donne le résultat. □

Passons à la preuve du théorème.

Démonstration. Démontrons le théorème par récurrence sur $n = |G|$.
Pour $n = 1$, le résultat est évident.
On suppose $n > 1$, notons N_1 l'exposant de G.

• Par le lemme précédent, il existe un élément $\chi_1 \in \widehat{G}$ d'ordre N_1. On a donc $\forall g \in G$, $\chi_1(g)^{N_1} = 1$.
Donc $\chi_1(G)$ est un sous-groupe des racines N_1-ièmes de l'unité et on a égalité car χ_1 est d'ordre exactement N_1.

Soit $x_1 \in G$ tel que $\chi_1(x_1) = \exp\left(\frac{2i\pi}{N_1}\right)$ et soit p l'ordre de x_1.
On sait que p divise N_1. Puis $\chi_1(x_1^p) = 1 = \exp\left(\frac{2ip\pi}{N_1}\right)$, donc N_1 divise p et finalement x_1 est d'ordre N_1.

• On pose $H_1 = \langle x_1 \rangle$. Montrons que $G \simeq H_1 \times \mathrm{Ker}(\chi_1)$. Comme $H_1 \simeq \mathbb{Z}/N_1\mathbb{Z}$ et $|\mathrm{Ker}(\chi_1)| < n$, on aura le résultat en appliquant l'hypothèse de récurrence.
En effet, si on décompose $\mathrm{Ker}(\chi_1)$ en $\prod_{i=2}^{r} \mathbb{Z}/N_i\mathbb{Z}$ avec $N_{i+1}|N_i$, alors comme les éléments de G sont d'ordre divisant N_1, on aura $G \simeq \prod_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}$ avec $N_{i+1}|N_i$.

χ_1 induit un morphisme surjectif α de H_1 sur $\mathbb{U}_{N_1}$, puis par égalité des cardinaux, α est un isomorphisme.
Soit $x \in G$, alors

$$x = \alpha^{-1}(\chi_1(x)) \left(\alpha^{-1}(\chi_1(x))\right)^{-1} x.$$

Par définition de α, $\alpha^{-1}(\chi_1(x)) \in H_1$.
Puis

$$\chi_1\left(\left(\alpha^{-1}(\chi_1(x))\right)^{-1} x\right) = \chi_1\left(\left(\alpha^{-1}(\chi_1(x))\right)^{-1}\right) \chi_1(x) = (\chi_1(x))^{-1}\chi_1(x) = 1,$$

donc $\left(\alpha^{-1}(\chi_1(x))\right)^{-1} x \in \mathrm{Ker}(\chi_1)$.
On a donc bien $G = H_1 \,\mathrm{Ker}(\chi_1)$.
On a aussi $H_1 \cap \mathrm{Ker}(\chi_1) = \{e\}$ car χ_1 est injectif sur H_1.
Il vient donc que $G \simeq H_1 \times \mathrm{Ker}(\chi_1)$, ce qui termine la preuve. □

Remarques : • On peut déduire de ce résultat le théorème de structure des groupes abéliens de type fini. On applique le théorème précédent au sous-groupe de torsion T, puis on peut prouver qu'on peut écrire $G \simeq T \times L$ avec L sans torsion. On montre en se donnant une base que L est isomorphe à $\mathbb{Z}^d$. Cela donne le résultat.
• Ce résultat peut être généralisé en le théorème de structure des modules de type fini sur les anneaux principaux.

Adapté du travail de Alexandre Bailleul.